ON THE TOTITIVES OF DIFFERENT ORDERS.

By Professor G. A. MILLER, Stanford University.

While the close connection between number theory and group theory has been frequently observed yet this connection has been explicitly developed in comparatively few cases. Such developments are especially important from a pedagogical standpoint since much time can be saved by studying related subjects from a common point of view. The following note aims to exhibit an interesting application of group theory to the totitives of different orders.

Let $\varphi(m)$ represent the number of natural numbers which are both prime to m and do not exceed m. The formula

$$\varphi(m)=m(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots\ldots\ldots(1-\frac{1}{p_n}),$$

$p_1, p_2, \ldots\ldots\ldots, p_n$ being the distinct primes which divide m, is known as Euler's φ formula. The value of $\varphi(m)$ is called the indicator of m, according to Cauchy. Sylvester has called it the totient of m, while the $\varphi(m)$ numbers themselves are called the totives of m. The formula has been generalized in a large number of ways.* Jordan,† Klein‡ and others have employed the following generalization.

Consider the number of different sets of k numbers such that none of these numbers exceeds m and that the greatest common divisor of m and all the numbers of any set is unity. The number of these sets is denoted by $\varphi_k(m)$ and is called the totient or indicator of order k with respect to m. When $k=1$ it reduces to the ordinary totient and the subscript is usually omitted. The value of $\varphi_k(m)$ may be determined as follows:

Suppose that an abelian group (G) has k independent generators $(s_1, s_2, \ldots\ldots\ldots, s_k)$ of order m. It is well known that every operator of G can be written in the form

$$s=s_1^{\alpha_1} s_2^{\alpha_2}\ldots\ldots\ldots s_k^{\alpha_k}, \quad \alpha_1, \alpha_2, \ldots\ldots\ldots, \alpha_k=1, 2, \ldots\ldots\ldots, m.$$

The order of s is m whenever the greatest common divisor of $m, \alpha_1, \alpha_2, \ldots\ldots\ldots, \alpha_k$ is unity, and conversely. Hence $\varphi_k(m)$ is equal to the numbers of operators of order m in G. To find this number it is convenient to consider a different set of independent generators of G. If

$$m=p_1^{\beta_1} p_2^{\beta_2}\ldots\ldots\ldots p_n^{\beta_n},$$

G is the direct product of n subgroups $(H_1, H_2, \ldots\ldots\ldots, H_n)$ of orders $p_1^{\beta_1 k}$,

*Cf. *Encyclopaedie der Mathematischen Wissenschaften*, Vol. 1, p. 557; Hagen, *Synopsis der Hoeheren Mathematik*, Vol. 1, p. 12; Lucas, *Theorie des Nombres*, Vol. 1, p. 399.

†Jordan, *Traite des Substitutions*, p. 96.

‡Klein-Fricke, *Theorie der Elliptischen Modufunctionen*, Vol. 1, p. 397.

$p_2^{\beta_2 k}$, ..., $p_n^{\beta_n k}$, respectively. Each of these subgroups has k independent operators of orders $p_1^{\beta_1}$, $p_2^{\beta_2}$, ..., $p_n^{\beta_n}$, respectively. These independent generators are also independent generators of G.*

In order to obtain an operator of order m it is necessary and sufficient that its factors from H_1, H_2, ..., H_n, respectively, be of the highest possible orders; *i. e.*, these factors must be of orders $p_1^{\beta_1}$, $p_2^{\beta_2}$, ..., $p_n^{\beta_n}$. The number of operators of $p_1^{\beta_1}$ in H_1 is clearly equal to its order diminished by the order of a group having its k invariants equal to $p_1^{\beta_1-1}$. As similar remarks apply to the other subgroups we have

$$\varphi_k(m)=p_1^{(\beta_1-1)k}\,p_2^{(\beta_2-1)k}\ldots\ldots p_n^{(\beta_n-1)k}\,(p_1^k-1)(p_2^k-1)\ldots\ldots(p_n^k-1)$$

$$=m^k\left(1-\frac{1}{p_1^k}\right)\left(1-\frac{1}{p_2^k}\right)\ldots\ldots\left(1-\frac{1}{p_n^k}\right).$$

It is well known that the $\varphi(m)$ numbers which are the totitives of m form a congruence group with respect to multiplication, viz., the group of isomorphisms of the cyclic group of order m. The total number of totitives of any higher order than the first do not form a group. If we take only those sets in which each of the k elements is prime to m we obtain $[\varphi(m)]^k$ sets which clearly form a group when the corresponding elements of the sets are multiplied together. This is the direct product of k groups of isomorphisms of the cyclic group of order m.

The above method of finding the value of $\varphi_k(m)$ is not any simpler than the one which does not involve the theory of abelian groups.† The main object of this note is to call attention to the fact that this important function is involved in the determination of the number of operators of highest order of some special type of abelian groups, while it is not difficult to determine the number of operators of every order in any abelian group.‡

From the standpoint of group theory the given $[\varphi(m)]^k$ sets of k numbers which are separately prime to m furnish an interesting extension of the important system of congruence groups formed by the totitives of m.§ It should however be observed that it is not possible to represent all abelian groups by such sets of numbers. All abelian groups having k invariants may however be represented as additive groups whose operators are sets of k numbers taken separately with respect to k mnduli m_1, m_2, ..., m_k, which are respectively equal to the invariants. In fact this is ordinarily done when the operators are represented by an index system.

*As the order of each of these nk independent generators is a power of some prime number these orders constitute the maximum number of invariants of G and they are completely determined by this property.

†Cf. *Theorie des Nombres*, 1900, p. 36.

‡Cf. Netto, *Vorlesungen ueber Algebra*, Vol. 2, 1900, p. 247.

§Weber, *Lehrbuch der Algebra*, Vol. 2 (1899), p. 60; Pund, *Mitteilungen der Mathematischen Gesellschaft in Hamburg*, Vol. 3 (1899), p. 371.